09/189,365.

DB Name	Query	Hit Count	Set Name
USPT	l3 and l4	2	L20
USPT	l13 and l14	0	L19
USPT	l14 same l15	0	L18
USPT	l14 same l15 same l16	0	L17
USPT	mapper	1297	L16
USPT	database	34093	L15
USPT	"Cool ICE"	481	L14
USPT	((707/$)!.CCLS.)	8685	L13
USPT	l3 same l10	1	L12
USPT	administator	9	L11
USPT	gateway	5555	L10
USPT	l6 and l8	16	L9
USPT	(service adj1 request) or messag$3	79408	L8
USPT	service adj1 request or messaging	7095	L7
USPT	l1 and (l3 or l4)	22	L6
USPT	l1 and l3 and l4	0	L5
USPT	script same (password or user-id or security)	202	L4
USPT	security adj1 profile	39	L3
USPT	Classic adj1 MAPPER	0	L2
USPT	(707/9 or 707/10 or 707/1 or 707/102)!.ccls.	2539	L1

09/189,365

DB Name	Query	Hit Count	Set Name
USPT	l1 and l18	2	L19
USPT	COOL adj1 ICE	560	L18
USPT	CLASSIC adj1 MAPPER	2	L17
USPT	MAPPER	1648	L16
USPT	l1 and l3	16	L15
USPT	l13 and l5	6	L14
USPT	(l4 same l6) and l1	20	L13
USPT	l4 same l5 same l6	1	L12
USPT	l2 same l3	2	L11
USPT	l9 and l1 and (l3 or l4) and l6	1	L10
USPT	l2 same l5	40	L9
USPT	l4 same l2 same l5	0	L8
USPT	l3 same l2 same l5	0	L7
USPT	(user-id or password or identification)	162391	L6
USPT	(first or second) near2 table	28049	L5
USPT	security same profile	1086	L4
USPT	security adj1 profile	69	L3
USPT	(request near4 access)	13393	L2
USPT	(707/9 OR 707/10 OR 709/203).CCLS.	2775	L1

WEST

End of Result Set

□ Generate Collection Print

L26: Entry 2 of 2 File: USPT Sep 11, 1990

DOCUMENT-IDENTIFIER: US 4956769 A
TITLE: Occurence and value based security system for computer databases

Abstract Text (1):
A method for providing an occurrence level, value based security protection system including the steps of building a data security table; extracting from the request to the database information concerning the system user, his terminal location, the data he wishes to access, and the operation he wishes to perform on the data; comparing these extracted pieces of information against the permitted access rules found in the data security table; returning a violation status to the host system making the request if the compared information fails to match the permitted access rules found in the data security table and logging the violation; permitting the execution of the request if the extracted data is found to match the permitted access rules found in the data security table.

Brief Summary Text (13):
The first of these tables is a data security access table. The data security access table has, for each data record and data field selected for security protection, a first entry identifying the data record or the data field and a second data security profile entry defining the Input/Output operations permitted on the data record or the data field identified by said first data security access table entry.

Brief Summary Text (14):
A second table that is established is a user security access table that has, for each user selected to have Input/Output access to the database, a first entry identifying the user and a second user security profile entry defining the Input/Output operations permitted on the database by the user identified by said first user security access table entry.

Brief Summary Text (15):
A third table that is established is a terminal location security access table that has, for each terminal location selected to have Input/Output operation access to the database, a first entry identifying the terminal location, and a second terminal location security profile entry defining the Input/Output operations permitted on the database from the terminal location identified by said first terminal location security access table entry.

Brief Summary Text (17):
A request table is built that has as its first entry the extracted userid, as its second entry the extracted subject data record and data field, as its third entry the extracted terminal location address, and, as its fourth entry, the extracted requested Input/Output operation.

Brief Summary Text (18):
The first request table entry for the userid is compared with the first entry of the user security access table and a first security condition "flag" is set to an "allowed" condition if a match is found and failing that, to a "violation" condition.

Brief Summary Text (19):
The fourth request table entry for the requested Input/Output operation is compared with the second entry of the user security access table whenever the first security

condition flag is in the "allowed" condition. If no match is found, the first security condition "flag" is set to a "violation" condition.

Brief Summary Text (20):
The second request table entry for the data record or data field entry, the subject of the Input/Output request that was parsed, is compared with the first data security access table entry and a second security condition flag is set to an "allowed" condition if a match is found and, failing that, to a "violation" condition.

Brief Summary Text (21):
The fourth request table entry for the requested Input/Output operation is compared with the second entry of the data security access table whenever the second security condition flag is in the "allowed" condition but if no match is found, the second security condition flag is set to a "violation" condition.

Brief Summary Text (22):
The third request table entry for the terminal location address is compared with the first terminal location security access table entry and a third security condition flag is set to an "allowed" condition if a match is found and to a "violation" condition if otherwise.

Brief Summary Text (23):
The fourth request table entry for the requested Input/Output operation is compared with the second entry of the terminal location security access table whenever the third security condition flag is in the "allowed" condition and the third security condition flag is set to a "violation" condition if no match is found.

Brief Summary Text (24):
The request table entries are then written to a security log database whenever any of the first, second or third security condition flag is in the "violation" condition. The execution of the parsed Input/Output request is cancelled by the host system. However, the Input/Output request is passed on to the host system for processing whenever the first, second and third security condition flags are in the "allowed" condition.

Detailed Description Text (7):
The preferred method of the present invention keeps the maintenance of use rules to a minimum by avoiding unnecessary redundancy and duplication using the concept of shared security profiles or access tables.

Detailed Description Text (8):
In general, the invention embodies the belief that a group of system users who have common work-related interest would also have a common "need to know" or access requirements on a particular database. Therefore, the security administrator of a host computer system would be able to define the majority of access privileges by the use of profiles or data access tables, that is a aset of user access rules shared by a group of users. Moreover, the concept was extended to allow an individual user to have multiple profiles within the host system. Demographically, the present invention is based upon the concept that the user community with the host system can be described topographically by defining the set(s) of group(s) to which a user belongs.

Detailed Description Text (9):
In the preferred embodiment of the present invention described below a given user can belong to a number of different profiles or data access tables. The exact number and membership of any one given user can be changed by the security systems programmer at the installation time of the value based security system described below as embodying the present invention.

Detailed Description Text (10):
In addition to user profiles, a given user can have a set of user specific access rules. These user specific rules are preferably very narrow in scope because the vast majority of significant generalizations will be defined witin the profiles. Profile access rules arè processed in preference to individual user specific rules. The present invention provides a method that will process all profiles while validating a request, and then if the request is still not satisified it will then process

individual user specific access rules if they are present.

Detailed Description Text (17):
Also, at system sign on by the user, a second user security access profile table is established for the subject system user.

Detailed Description Text (18):
This second user security access profile table defines, for each user selected to have authorized access for performing Input/Output operations on the database, a first entry identifying the unique user identification symbol of the selected user, and a second entry associated with the first entry that defines the Input/Output operations permitted on the database by each user identified by the first user security access profile table entry.

Detailed Description Text (21):
Specifically, the user access profile table and the terminal location security access table are constructed within the host system environment by parsing the system sign-on by the system user and extracting therefrom the unique user identification symbol.

Detailed Description Text (26):
Using these parsed requests, an Input/Output operations request table is built having as its first entry the unique user identification symbol of the system user making the Input/Output operation request, as its second entry the data record and data field that is the object of the Input/Output operation request being parsed, as its third entry the terminal location address from which the Input/Output operation request is being made, and, as its fourth entry the entered Input/Output operation request being made.

Detailed Description Text (40):
In order to accomplish this, the data security access table, the user security access profile table and the terminal location security access table are retained within the host system until the system user terminates the session with the host computer system, that is logs off the system.

Current US Original Classification (1):
707/9

CLAIMS:

1. In a computer host system interfacing Input/Output requests between at least one system user identified by a unique user identification symbol that is accessing the host system from at least one terminal location having a unique terminal address, and the host system having at least one database having data records, including data fields, a method for providing occurrence level, value based security protection, limiting to selected users and terminal locations access to preselected, but variable Input/Output operations on selected data records and data fields of the databases, comprising the steps of:

(a) establishing at said computer host system a data security access table having, for each data record and data field selected for security protection, a first entry identifying the data record and the data field and a second entry representing a data security profile associated therewith, said second entry defining the Input/Output operations permitted on the the data record and data field identified by said associated first entry;

(b) establishing at said computer host system a user security access table having, for each user selected to have Input/Output access to the database, a first entry identifying the user and a second entry representing a user security profile associated therewith, said second entry defining the Input/Output operations permitted on the database by the user identified by said associated first entry;

(c) establishing at said computer host system a terminal location security access table having, for each terminal location selected to have Input/Output operation access to the database, a first entry identifying the terminal location and a second entry representing a terminal location security profile associated therewith, said second entry defining the Input/Output operations permitted on the database from the terminal location identified by said associated first entry;

(d) parsing each Input/Output request from the host system to the database and extracting therefrom: (1) the unique user identification symbol of the system user making the Input/Output request; (2) the data record or data field that is the subject of the Input/Output request; (3) the terminal location address from which the Input/Output request is being made; and, (4) the requested Input/Output operation;

(e) building at said computer host system a request table having as its first entry the extracted unique user identification symbol, as its second entry the extracted subject data record and data field, as its third entry the extracted terminal location address, and as its fourth entry the extracted requested Input/Output operation;

(f) comparing said first request table entry for the unique user identification symbol with the first entry of the user security access table and setting at said computer host system a first security condition "flag" to an "allowed" condition if a match is found and otherwise to a "violation" condition;

(g) comparing said fourth request table entry for the requested Input/Output operation with said second entry of said user security access table whenever said first security condition "flag" is in said "allowed" condition and setting said first security condition "flag" to a "violation" condition if no match is found;

(h) comparing said second request table entry for the data record or data field entry that is the subject of the Input/Output request with the first data security access table entry and setting at said computer host system a second security condition "flag" to an "allowed" condition if a match is found and otherwise to a "violation" condition;

(i) comparing said fourth request table entry for the requested Input/Output operation with said second entry of said data security access table whenever said second security condition "flag" is in said "allowed" condition and setting said second security condition "flag" to a "violation" condition if no match is found;

(j) comparing said third request table entry for the terminal location address with the first terminal location security access table entry and setting at said computer host system a third security condition "flag" to an "allowed" condition if a match is found and to a "violation" condition otherwise;

(k) comparing said fourth request table entry for the requested Input/Output operation with said second entry of said terminal location security access table whenever said third security condition "flag" is in said "allowed" condition and setting said third security condition "flag" to a "violation" condition if no match is found;

(l) writing at said computer host system said request table entries to a security log database whenever said first, second or third security condition "flag" is in said "violation" condition and cancelling the execution of the parsed Input/Output request by the host system;

(m) returning the Input/Output request to the host system for processing whenever said first, second and third security condition "flag" is not in said "violation" condition.

2. In a computer host system interfacing Input/Output requests between at least one system user identified by a unique user identification symbol that is accessing the host system from at least one terminal location having a unique terminal address, the host system further having at least one database having data records, including data fields, a method for providing occurrence level, value based security protection, limiting to selected users and terminal locations, access to preselected, but variable Input/Output operations on selected data records and data fields of the databases, the method comprising the steps of:

(a) establishing at said computer host system at system sign on by the system user, a data security access table for the system user having, for each data record and data field selected for security protection, a first entry identifying the data record and data field and a second entry associated with said first entry, defining the Input/Output operations permitted on the data record and data field identified by said associated first entry;

(b) establishing at said computer host system at system sign on by the system user, a user security access profile table for the system user having, for each user selected to have authorized access for performing Input/Output operations on the database, a first entry identifying the unique user identification symbol of the selected user, and a second entry representing a user security profile associated with said first user security access profile table entry, said second entry defining the Input/Output operations permitted on the database by the user identified by said associated first entry;

(c) establishing at said computer host system a terminal location security access table having, for each terminal location selected to have access for performing Input/Output operations on the database, a first entry identifying the terminal location and a second entry representing a terminal location security profile associated with said first terminal location security access table entry, said second entry defining the Input/Output operations permitted on the database for the terminal location identified by said associated first entry;

(d) parsing each Input/Output operation request from the host system to the database and building at said computer host system an Input/Output operations request table having as its first entry the unique user identification symbol of the system user making the Input/Output operation request, as its second entry the data record and data field that is the object of the Input/Output operation request being parsed, as its third entry the terminal location address from which the Input/Output operation request is being made, and, as its fourth entry the entered Input/Output operation request being made;

(e) comparing sequentially each of said data entry elements of said Input/Output operation request table with its said corresponding data entry element of said user security access table, said data security access table, and said terminal location security access table, respectively, for setting at said computer host system a corresponding "flag" to an "allowed" or "violation" condition in the event of a match or no match being found between corresponding data entry elements being compared respectively;

(f) writing at said computer host system said Input/Output operation request table entries to a security violation log database whenever at least one of said "flags" corresponding to said Input/Output operation request table entries is in said "violation" condition and cancelling the execution of the parsed Input/Output operation request from the host system; and,

(g) returning the parsed Input/Output operation request to the host system for processing whenever all of said "flags" corresponding to said Input/Output operation request table entries are in said "allowed" condition.

3. A method as in claim 2 further including the step of retaining said data security access table, said user security access profile table and said terminal location security access table until the system user logs off the host computer system.

4. A method as in claim 3 wherein said step of establishing said data security access table, said user access profile table an said terminal location security access table, each includes the steps of:

(i) parsing the system sign on by the system user and extracting therefrom the unique user identification symbol;

(ii) building each of said respective tables by comparing said extracted unique user identification symbol against a value based security database having for each unique user identification symbol a first entry representing the unique user identification symbol and a second entry containing a selected set of access rules associated with said first entry for determining allowable Input/Output operations by the system user